

Erklärung zur Datensicherheit

I. Datenschutz bei der Nutzung des KDN III

Das KDN III wird als geschlossene Benutzergruppe für alle sächsischen Kommunalverwaltungen und Einrichtungen mit kommunalem Bezug bereitgestellt. Alle für kommunale Belange notwendigen Übergänge in andere Netze werden nach den Regeln des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geschützt. Zum Schutz des eigenen lokalen Netzes des Netzkunden und zur Vermeidung einer Gefährdung der geschlossenen Benutzergruppe von innen durch einzelne angeschlossene Verwaltungen und Einrichtungen sind bei der Nutzung der Dienste des KDN III Schutzmaßnahmen seitens des Netzkunden erforderlich.

Nachfolgende Regelungen dienen dazu, die an das KDN III angeschlossenen Netzkunden vor

- unberechtigter Kenntnisnahme (Verlust der Vertraulichkeit),
- unberechtigter Veränderung oder Verfälschung (Verlust der Integrität) und
- Beeinträchtigung oder Verlust der Verfügbarkeit (Verlust der Funktionalität)

ihrer Daten zu schützen.

II. Folgende drei Varianten externer Netzübergänge sind (je nach örtlicher Gegebenheit) denkbar:

Der Netzkunde hat

- 1) nur einen Zugang zum KDN III, über den sowohl der Zugang zum Internet als auch die Übergänge in Netze Dritter erfolgen,
- 2) einen Zugang zum KDN III, nutzt jedoch einen separaten Einzelplatz-PC bzw. ein separates LAN für den Zugang zu Netzen Dritter,
- 3) neben dem Zugang zum KDN III nicht über das KDN III geführte Zugänge zu Netzen Dritter.

Unabhängig von der Anschlussvariante hat der Netzkunde alle erforderlichen und angemessenen Schutzmaßnahmen nach § 9 SächsDSG zu ergreifen. Darüber hinaus sind nachfolgend beschriebene Sicherheitsanforderungen einzuhalten:

zu 1)

Aus dem lokalen Datennetz (LAN) werden keine weiteren Übergänge in Netze Dritter betrieben oder für den Betrieb bereitgehalten und werden auch in Zukunft nicht bereitgestellt werden. Ein eigener Übergang vom LAN ins Internet ist ausgeschlossen. Derartige Übergänge dürfen nur mit Zustimmung der KDN GmbH geschaffen werden. Sollten solche Übergänge erforderlich werden, dann werden diese nur nach gemeinsamer Absprache und entsprechend der von der KDN GmbH geforderten Schutzmaßnahmen (Testierung des Schutzes ist notwendig) eingerichtet.

zu 2)

Durch die physikalische Trennung KDN III und dem Zugang zu Netzen Dritter bestehen keine speziellen Anforderungen an zusätzliche Sicherheit.

zu 3)

Der Netzkunde hat weitere, nicht über das KDN III geführte, separate Zugänge zu Netzen Dritter. Alle IT - Verfahren sind in einem Sicherheitskonzept mit ihrer Schutzwürdigkeit und den zum Schutz des eigenen lokalen Netzes des Netzkunden, des KDN III und aller an das KDN III angeschlossenen Kommunalverwaltungen und Einrichtungen ergriffenen Sicherheitsmaßnahmen zu beschreiben.

Mindestanforderung für einen Parallelbetrieb von Zugängen zum KDN III und zu separaten Dritten ist die Realisierung eines Firewallschutzes zwischen dem LAN des Netzkunden, dem KDN III und dem Netz des/der Dritten. Hierfür kann ein mehrstufiges Firewallsystem mit Paketfilter, Applicationgateway und Screeningrouter erforderlich werden, das von ausgebildetem Personal des Netzkunden laufend überwacht und auf dem jeweils neuesten Stand gehalten werden muss. Das Firewallsystem muss die Sicherheitsstandards der jeweils gültigen Fassung der IT - Grundschieckataloge des BSI erfüllen. Dieser Netzübergang ist in seiner Gesamtheit als Verfahren mit hohem Schutzbedarf einzustufen. Der Netzkunde erbringt durch Testierung der im Sicherheitskonzept dargestellten Maßnahmen zum Schutz des KDN III den Nachweis gegenüber der KDN GmbH.

III. Erklärung des Antragstellers (Netzkunden)

Die Netzwerkanbindungen in unserer Verwaltung entsprechen der unter Punkt II. genannten Variante: (bitte ankreuzen)

1)

2)

3)

Wir erklären uns bereit, die zu der jeweils zutreffenden Variante erforderlichen Sicherheitsmaßnahmen einzuhalten und mögliche Veränderungen an unseren Einrichtungen unverzüglich mitzuteilen. Wir verpflichten uns zudem, sofern nicht bereits vorhanden, ein IT - Sicherheitskonzept zu erstellen und zu aktualisieren sowie übergreifende Maßnahmen zur Sicherheit der Informationstechnik in speziellen Regelungen (Dienstordnung, Dienstvereinbarung für Internet bzw. E-Mail usw.) verbindlich festzulegen. Insbesondere werden Regelungen über Zugangsberechtigungen, Benutzerkontrolle, Zugriffsberechtigungen, Übermittlungskontrolle sowie Weitergabe, Verwendung und Transport von Daten getroffen und die diesbezüglichen Verantwortlichkeiten in entsprechenden Dienstanweisungen festgelegt. Die Vorgaben des SächsDSG bzw. BDSG werden von uns eingehalten.

Nur bei Variante 3) gefordert:

1. Die laut Sicherheitskonzept zum Schutz des KDN III ergriffenen Maßnahmen wurden testiert.¹
2. Es ist ein Testat angelehnt an das „Prüfschema für die Erteilung eines Testats nach der Basis-Absicherung gemäß IT-Grundschutz“ des BSI durch einen beim BSI lizenzierten IT-Grundschutz-Auditor zu erstellen. Die Stichprobe muss dabei die Bausteine NET.3.1 und NET.3.2 sowie alle Baustein-Zielobjekte umfassen, welche den Netzübergang zwischen KDN, LAN und den Netzen Dritter abbilden. Es sind dabei die Standard-Anforderungen zu prüfen.
3. Das Sicherheitsniveau der testierten Fremdnetz-Übergänge wird von uns durch geeignetes Personal dauerhaft aufrechterhalten.
4. Bei geplanten neuen Fremdnetz-Übergängen werden wir vor deren Realisierung eine neue Testierung veranlassen und die KDN GmbH unverzüglich darüber unterrichten.
5. Wir sind bereit, durch die KDN GmbH veranlasste Sicherheitsüberprüfungen durchführen zu lassen.
6. Wir wiederholen die Testierung regelmäßig, spätestens jedoch unmittelbar nach Ablauf der Gültigkeit der Testierung und in jedem Fall bei Änderungen am IT – Verbund gemäß Ziffer 2.

Das Testat durch einen vom BSI lizenzierten Auditor ist beigelegt.

Uns ist bekannt, dass wir bei Nichteinhaltung der Anforderungen aus dieser Sicherheitserklärung das eigene lokale Netz sowie die geschlossene Benutzergruppe und das KDN III gefährden und für alle hierdurch mutwillig oder fahrlässig verursachten Schäden haften und die KDN GmbH zur außerordentlichen, fristlosen Kündigung berechtigt ist.

Der Zugang zum KDN III und zum Sächsischen Verwaltungsnetz (SVN 2.0) kann durch die KDN GmbH bei Bekanntwerden eines vom Netzkunden ausgehenden Sicherheitsvorfalls ohne Angabe von Gründen oder einer vorherigen Benachrichtigung gesperrt werden.

Dies vorausgeschickt, bestätigen wir hiermit vorstehende Erklärung zur Datensicherheit.

Ort, Datum

gesetzlicher Vertreter Antragsteller (Netzkunde)

¹ Sofern die Testierung zum Zeitpunkt der Anschlussbeauftragung noch nicht abgeschlossen wurde, ist der voraussichtliche Zeitpunkt mitzuteilen und die Testierung nachzureichen.